March 2021

RAPID RECORDING OF NON-TAMPERED FAILURE CONDITIONS

HP INC

Rapid Recording of Non-Tampered Failure Conditions

Abstract: A mechanism for an electrical device measures device stress and keeps track of failure conditions in a non-tamperable manner. The measurements can be retrieved even if the device is dead and used to determine if the failure was caused by environmental factors.

This disclosure relates to the field of electronic devices.

A technique is disclosed that measures stress in an electrical device and keeps track of failure conditions faster than writing them in a log, and in such a way that they can be retrieved without a network connection even if the device is dead.

Device failures often stem from poor quality of the electricity provided in certain parts of the world, or in certain electrically stressed environment. Devices that have been built to function within certain power limits can break when the power exceeds these limits. But when customers see an abnormal rate of hardware failures they typically complain to the manufacturer about the device quality rather than blaming their own environment for the failure. Such manufacturers also have a hard time proving that their environmental conditions were at fault. They typically must ship expensive measuring equipment to monitor these environments over a long period of time, and subsequently dispatch engineers to exploit results before the root cause can be identified as the environment rather than the devices.

According to the present disclosure, and as understood with reference to the Figure, electrical stresses (electrical source anomalies) are sensed by a device 10 and recorded even in the case of rapid device death (e.g. due to electrical surges), and in a way that the failure cause can be retrieved even when the device is dead and while establishing proof of the stress conditions that caused the failure.

Such a device includes a hardware component 20 that monitors electrical conditions (e.g. voltage levels) and at least counts (or better logs) events versus at least a configured threshold. It also includes a set of one-time non-replaceable fuses and various resistances. It further includes an RFID black box 30 able to store at least the counter and/or at least some portion of the when the device 10 is functional, such that it may be retrieved after the device 10 has failed and is dead. In addition, the device 10 can get enough energy from its primary RFID antenna 40 to read and provide the impedance of the combined fuses 52, 54, 56 in the system. Alternatively or additionally, the device 10 has a modular antenna 60 functioning at various impedances determined by fused fuses. A corresponding RFID reader 70 is able to scan various frequencies until the answer of the RFID on one of these frequencies will help determine which fuses are fused and which are not fused.

When the device 10 is functional, the controller ("C") may access the counter, or log 20 and report on it via classical telemetry, and may thus detect when electrical inputs are above expected levels but haven’t yet impacted the operation of the device 10. This may include fusing a tracking fuse calibrated with expected threshold with regards to the actual strength of the device 10 itself.

If the device 10 is dead, the external RFID reader 70 can bring the energy required to the black box 20 via its RFID regular antenna 40, and activate the RFID chip logic to measure and provide the impedance remaining in the combined fuse system 52, 54, 56.

Alternatively, the reader 70 can emit on various frequencies until the RFID answers, thus identifying which fuse(s) are left in the antenna 60 (when the fuses are part of that antenna). A combination of both techniques may also be used.

In case of a rapid surge, the controller ("C") may not have time to record its level in the black box 20. But fuse 54 (and possibly fuse 56), if fused, will give an indication of that surge. By reading the black box content and by understanding which fuse 52, 54, 56 is blown, the reader 70 will have enough information to conclude that the death of the device 10 was caused by an electrical surge.

This solution can be extended to other conditions of electrical over-stress or any other type of environmental stress that may kill a device before it could record the reason of its death. It can be added to any electric device and/or its respective power adaptor, and/or even to electrical plugs (male or female).

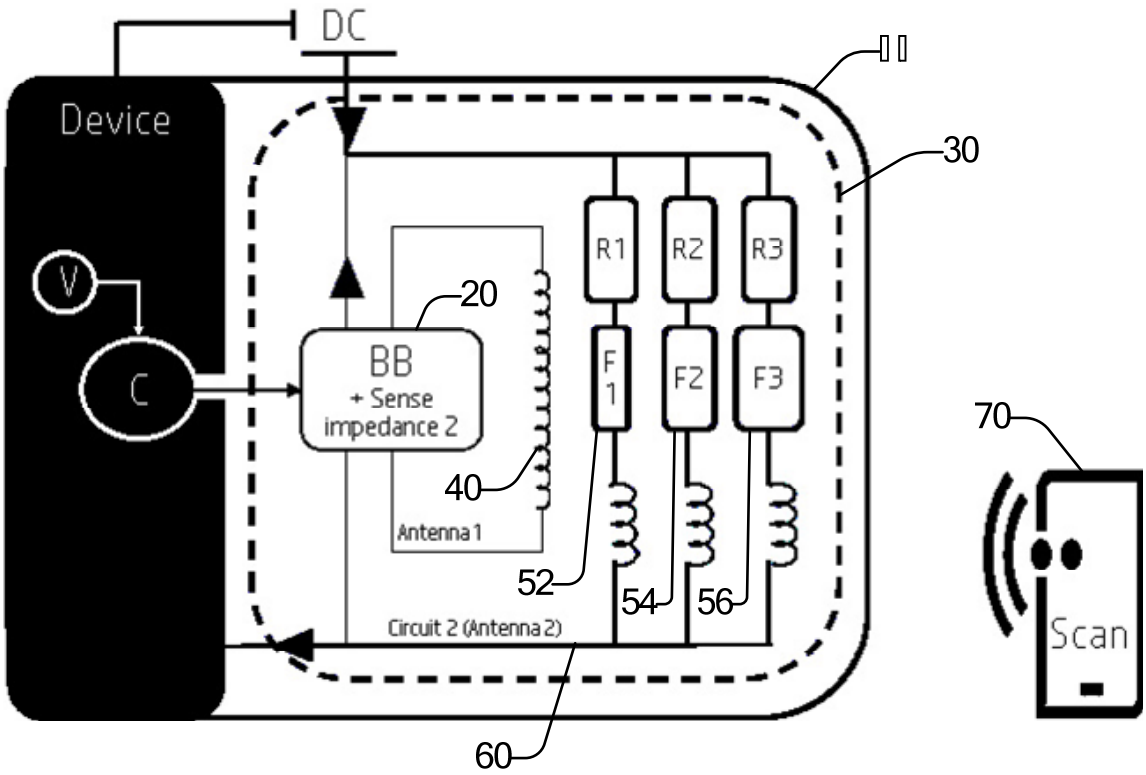
A mechanism according to the disclosure can be embedded in the structure of a 3D-printed object, without requiring more space than the original object. For example, electrical elements such as fuses and antennas may be 3D-printed in the structure of a power adapter using conductive inks or other materials. Tuning the resistivity (or conductivity) is possible by controlling the addition of a conductive agent and a resistive agent in the ink or material. Then a resistor with a fixed resistance can be designed by choosing a specific resistivity combination and trace dimension. If the current and voltage limits of a system are known, a 3D-printed fuse can be designed to break at currents or voltages outside of the designed parameters. When the fuse experiences a current or voltage outside of its spec, it may break the trace or change the resistance of the fuse. Both mechanisms can be identified by the appropriate circuitry to indicate to the system that a fault has detected. This resistance change would load an RFID antenna circuit and detune the impedance and cause the signal strength to change.

The technique can be deployed in a manner that makes it tamper-resistant. The design topology of the 3D circuitry may be adapted in a random manner in each device such that by not knowing how it is built it would become very hard to detect. This inhibits tampering with the failure detection mechanism and helps prevent fraudulent claims.

The disclosed technique may also be deployed in a peripheral such as a docking station, a power adapter, or a power plug that logs environmental stress as a proof of what may have likely caused an issue on an attached device. Disposing such devices on a certain percentage of powered points in a floor may suffice to infer if the environment may be the source of a device class issue occurring on that floor.

The disclosed technique advantageously provides inexpensive forensics into electrical causes of device failure, as a user with a smartphone may use it to harvest the failure information from the devices that have failed, and the fuse status which may indicate why it failed. The ease of acquiring such failure information allows users to more easily evaluate whether these failures were due to their environmental conditions, rather than some defect in the failed device itself.

Disclosed by Patrick Jacques Andre Marie De Marcillac, Sandro Secci, Rudolf Wegener, and Jarrid Wittkopf, HP Inc.


DC
Device
V
C
BB
+ Sense
impedance 2
20
30
R1
R2
R3
F1
F2
F3
40
Antenna 1
52
54
56
Circuit 2 (Antenna 2)
60
70
Scan